EXHIBIT 81

Redacted Version of Document Sought to be Sealed

Message

From:	Ramin Halavati [rhalavati@google.com]
Sent:	8/8/2019 1:40:33 PM
To:	Sammit Adhya [sammit@google.com]
CC:	Florian Uunk [feuunk@google.com]; Sabine Borsay [sabineb@google.com]; Rory McClelland [rorymcclelland@google.com]; Greg Fair [gregfair@google.com]; Burton Rast [rast@google.com]
Subject:	Re: SinRastro / Chrome

Hi Sammit,

Thanks a lot for the explanation, I totally agree that presenting a simpler and more clear user story would be a user trust gain.
Let's continue the discussion on alternatives in the next week's meeting.

Best,
Ramin

On Thu, Aug 8, 2019 at 6:29 AM Sammit Adhya <sammit@google.com> wrote:
Hi Ramin,

Thanks for continuing to be so thoughtful about this. I definitely understand the risks of walking back on this narrative. At a high level, what we're really trying to address is the risk of a user who prefers to be private having their privacy actually eroded through data collection because we don't know of their intention to be private. Assuming we can solve the PR narrative, I believe that preventing the data collection is better for the user and we should be able to tell that story in a way that users understand.

To be perfectly clear, the data collected while Incognito is strictly **NOT** anonymous. When using a Google service, data (e.g. search queries) is tied to a pseudonymous ID (e.g. zwieback) that is then stored with the user's IP address, user agent, and other metadata (everything in the gwslog proto). While we don't connect it to a user's identity and there are many internal policies to ensure it does not happen, it's not impossible. Further, under the GDPR, data tied to unauthenticated identifiers **IS** considered to be personal data. See GDPR analysis here. That means everything a user does while signed out of Google services is considered to be personal data.

In terms of users' perception, there are dozens of articles that discuss the fact that Incognito is not really all that private because of the data collected while using it, and some that point out that Google is still "tracking you". Here's a sample:

- Google Denies Tracking People Through Incognito Mode - But Doesn't Say It's Not Possible
- Google Chrome's Incognito Mode is way less private than you think
- Google Chrome's Incognito Mode may not be as private as you think
- Chrome's anonymous browsing feature isn't as secret as we assumed
- Google denies claim that it's tracking internet users when incognito mode is on
- Why should I use DuckDuckGo while Google in Incognito does the same thing? (Quora)

Realize that some of these are misconceptions and some are inaccurate, but that is kind of irrelevant. It's about the perception. Imagine being able to make the promise that if you use Google services while Incognito, we won't save your data. Period. That is an incredibly powerful statement for a company like Google to make. Of course, users may not understand some of these distinctions and maybe they won't understand the benefit, but I believe it is in their best interest.

Additionally, this battle of "detecting Incognito" seems like it will be never ending.. sounds like there is research attempting to work around the fix in 76 [method 1, method 2]. That's not to say these work, or we can't accomplish this, but we potentially might be continuously trying to stay ahead, while making privacy worse by collecting Incognito when the user has clearly told Chrome that it wants to be private. That is the fundamental reason for trying to strengthen Incognito and allow Google services to actually deliver on the promise of being private.

Let's continue chatting about the other concerns at our sync next week as well as next steps. Hopefully this helps levelset on the user benefit. I'm also trying to find some time with comms/PR/policy so we can walk through how we might approach that aspect.

Thanks again,
Sammit

On Tue, Aug 6, 2019 at 5:47 AM Ramin Halavati <rhalavati@google.com> wrote:
 Hi Sammit,

3) Having the NTP solution as a just-in-time control might be hard, and if users are not opted in to 3rd party cookie blocking and have previously opened tabs, there might be leakage risks on changing this toggle's state. But this is something that we can work on the details and assess the risks and maybe warn user accordingly. But given that this is already a complicated issue to communicate to users, it seems safer to stay on the simpler side.

4) Sorry to jump back to this issue but I discussed the proposals today with Chrome privacy team and I think that to convince Chrome team about the letting-websites-know solution, we definitely need a good answer to the following two questions:

1.   Why this is beneficial for the users and knowing that Google gets anonymous ids in incognito and they are no way connected to users' identities, how can we tell users that this is done for their benefit?

2.   What would be the PR narrative that doesn't damage Chrome's user trust, when a few months ago we strongly defended private-browsing's anonymity and now we are changing the case.

I **strongly** believe that if we proceed to steering committee and even if they approve either of these letting-websites-know approaches, we would get the push back from Chrome team later, so it's better to work through these issues first and have an initial answer for them. This would be much more severe if we go towards a default-on approach where users just have the option to opt-out.

5) Can we have a more clear representation of regulator's requirement? Do they really care if Google stops logging anything in Chrome incognito mode or private browsing in general? Current approach is quite Chrome browser specific and if we won't have the feature as default-on (which requires item 4) the most we can get is an option for users to tell Google they don't want logging.

Thanks,

GOOG-CABR-00501221

Ramin

P.S. Here are two articles defending keeping private-browsing hidden:
   What Chrome's Incognito changes mean to the metered paywall vs. freemium debate
   Chrome 76 and the End of the Incognito Loophole

On Tue, Aug 6, 2019 at 4:22 AM Sammit Adhya <sammit@google.com> wrote:
   Hi Ramin,

   What would be the downside to blocking 3p cookies while Incognito? ████████████████
   ████████████████████████████

   Having a toggle on the NTP page as a "just-in-time" control that is only valid for the session is also
   interesting. ██████████████████████████████

   Thanks,
   Sammit

On Mon, Aug 5, 2019 at 3:57 AM Ramin Halavati <rhalavati@google.com> wrote:
   Hi All,

   ██
   ██
   ██

   ██
   ██

   What do you think?

   Best,
   Ramin

On Mon, Aug 5, 2019 at 8:13 AM Sammit Adhya <sammit@google.com> wrote:
   Hi All,

   Just wanted to circle back here based on the conversation with Ramin last week.

   ██
   ████████████████████████████████████ I added a slide with some pros and cons so PTAL. Both
   seem like reasonable options so let's continue to get feedback. I'll also set up some time with our
   comms/policy folks to better understand what an option like this could mean and if there's a narrative that
   might work. Will include martinal@ in that conversation.

   Thanks so much for the continued thoughtfulness on thinking through these proposals!

   Best,
   Sammit

On Tue, Jul 30, 2019 at 6:25 AM Ramin Halavati <rhalavati@google.com> wrote:
Hi Sammit,

Thanks, let's continue the discussion in today's meeting. My general concern for the approach is:

• Since many websites may start adding this permission request, we need to add a way for users to dismiss spamming permission requests, which most probably would include an option to "Say no to all".

• Expecting that most users go with this easy option and don't fine tune it for different websites, I don't expect Google would also receive that much positive answer.

• Therefore, instead of the expected result of *"Going to incognito mode stops Google logging in all products"*, we would have *"Users have a way to set up Incognito to tell Google to stop logging for all products"*. This is not what Sundar promised.

Hence I see the solution mostly as a remedy for Google to tell regulators that we gave the option to the users, but they didn't use it, and not a feature for the users.
And if we really want to have a solution that gives the first promise, we should find a way to go through the PR issues of it and set this feature on-by-default, removing websites need to ask request to know, and provide users an approach to hide it from some/all websites.

Best,
Ramin

On Mon, Jul 29, 2019 at 8:03 AM Sammit Adhya <sammit@google.com> wrote:
+Steve Hamilton (PDPO UXR) as FYI

Hi Ramin,

Sorry for the delay! Answers inline below.

Thanks,
Sammit

On Fri, Jul 26, 2019 at 1:05 AM Ramin Halavati <rhalavati@google.com> wrote:
Hi,

And another question that popped up while working on the design spec of this proposal: What is the main problem that we want to solve with the new Sin Rastro proposal?
Is it just *"Google websites want to be able to distinguish new users from private-browsing users, so that they stop logging in private-browsing"*, or I am missing something?
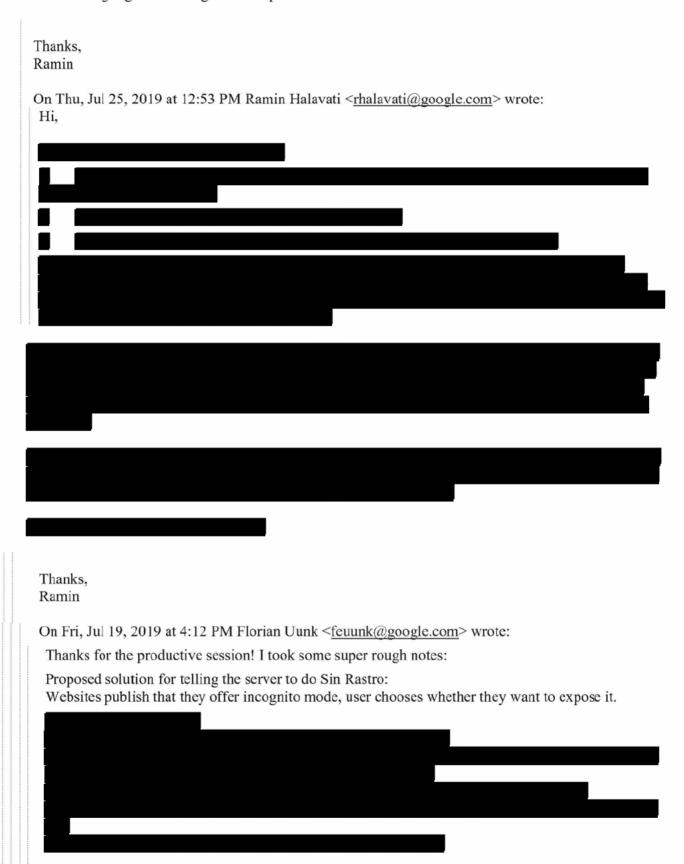If that's all, can we describe it as a user problem instead of Google problem and say what would be the benefit for users and to get what, would they say yes to a prompt to let the website know they are in private browsing?

That's definitely one of the bigger problems we're trying to solve (largely because this is the space that we have direct control over).

>From an ecosystem perspective, do you think 3p websites would want to be more proactive when Incognito? Is there a world where we have a W3C spec that defines what it means for a website to support Incognito? If so, then the problem extends beyond just Google websites.

In the long-run, ideally, we move towards a world where we do this by default for signed out users. We'll be sure to highlight that being another option.

Thanks,
Ramin

On Thu, Jul 25, 2019 at 12:53 PM Ramin Halavati <rhalavati@google.com> wrote:
Hi,

Thanks,
Ramin

On Fri, Jul 19, 2019 at 4:12 PM Florian Uunk <feuunk@google.com> wrote:

Thanks for the productive session! I took some super rough notes:

Proposed solution for telling the server to do Sin Rastro:
Websites publish that they offer incognito mode, user chooses whether they want to expose it.

████████████████████

Spaces overlap:
We'll work on notifications for any sign-in in incognito
When can we block sign-ins to Google? Need profile creation and usage in usable state first

What about incognito vs. Guest
We could make the default for incognito to not bring data.
Would be more aligned with native app incognito modes.
Would have to keep the functionality of bringing your data along, just moving it.
Proposal: do not bring data, and merge guest mode into incognito?
Could have a setting to bring in the data on the incognito NTP?

SinRastro / Chrome

When	Fri 19 Jul 2019 13:00 – 17:00 Central European Time - Berlin
Where	MUC-ARP-3Z0-Seaview (8) [GVC] (map)
Joining info	**Redacted - Privacy** More phone numbers
Who	• Ramin Halavati- organiser
	• Rory McClelland
	• Sammit Adhya
	• Greg Fair
	• Florian Uunk - optional
	• rast@google.com - optional
	• Sabine Borsay - optional

--

Sammit Adhya | Privacy and Data Protection | sammit@google.com | (650) 253-3001

--

Sammit Adhya | Privacy and Data Protection | sammit@google.com | (650) 253-3001

--

Sammit Adhya | Privacy and Data Protection | sammit@google.com | (650) 253-3001

--

Sammit Adhya | Privacy and Data Protection | sammit@google.com | (650) 253-3001

PRODBEG: GOOG-CALH-00452518
PRODBEGATT:
PRODEND: GOOG-CALH-00452524
PRODENDATT:
PRODVOL: CROSS-PROD002
2nd_CROSS_BEGBATES:
2nd_CROSS_ENDBATES:
AllCustodians: Florian Uunk;Greg Fair
TO: sammit adhya <sammit@google.com>
FROM: ramin halavati <rhalavati@google.com>
CC: sabine borsay <sabineb@google.com>;florian uunk <feuunk@google.com>;rory mcc-
        lelland <rorymcclelland@google.com>;burton rast <rast@google.com>-
        ;greg fair <gregfair@google.com>
BCC:
CONFIDENTIALITY: CONFIDENTIAL
CROSS_ALLCUSTODIANS:
CROSS_ATTACHMENTNAME:
CROSS_BEGATTACH:
CROSS_BEGBATES: GOOG-CABR-00501220
CROSS_CC:
CROSS_CONFIDENTIALITY:
CROSS_CUSTODIAN:
CROSS_DATECREATED:
CROSS_DATEMOD:
CROSS_DATERECEIVED:
CROSS_DATESENT:
CROSS_DE-DUPED CUSTODIANS:
CROSS_ENDATTACH:
CROSS_ENDBATES: GOOG-CABR-00501226
CROSS_FILEEXTENSION:
CROSS_FILENAME:
CROSS_FROM:
CROSS_MD5 HASH:
CROSS_MESSAGE ID:
CROSS_OWNER:
CROSS_PRODVAL:
CROSS_REDACTED:
CROSS_SUBJECT:
CROSS_TITLE:
CROSS_TO:
CUSTODIAN/SOURCE: Greg Fair
DATECREATED:
DATELASTMOD: 08/08/2019
DATERCVD: 08/08/2019
DATESENT: 08/08/2019
DeDupedCustodians: Florian Uunk;Greg Fair
DOCEXT: eml
FILENAME:
ILS_ProdDate: 09/01/2021
CROSS_ILS_ProdDate: 09/01/2021
MD5 HASH: D1DAF97F975FC8862D5BAD079BF2D73F
MessageID: <CAORodQiMFEHGeoNcGg4JzhYqjfVKDSUsGNuk=qEAdM2uU5VD4Q@mail.gmail.com>
NATIVEFILE:
Owner: rhalavati
PAGES: 7

REDACTED: Y
SUBJECT: Re: SinRastro / Chrome